



Attorney Docket No. 915-008.022
Serial No. 10/804,852

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

In Re Application of:

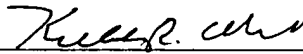
Lauri PAATERO : Confirmation No. **7439**
Serial No: **10/804,852** : Examiner: **Andrew NALVEN**
Filed: **March 19, 2004** : Group Art Unit: **2134**

For: **PRACTICAL AND SECURE STORAGE ENCRYPTION**

Mail Stop Appeal Briefs-Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

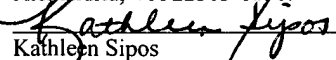
APPEAL BRIEF

Submitted by:



Keith R. Obert
Attorney for Appellant
Registration No. 58,051
WARE, FRESSOLA, VAN DER SLUYS &
ADOLPHSON, LLP
755 Main Street, PO Box 224
Monroe, CT 06468
Telephone: 203-261-1234

I hereby certify that this paper is being deposited with the U.S.
Postal Service on the date shown below with sufficient postage
as first class mail in an envelope addressed to: Mail Stop Appeal
Briefs-Patents, Commissioner for Patents, P.O. Box 1450,
Alexandria, VA 22313-1450.


Kathleen Sipos
Date Feb. 5, 2009

02/10/2009 LNGUYEN1 00000017 10004052

01 FC:1402

540.00 OP



IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

In Re Application of:

Lauri PAATERO : Confirmation No. **7439**
Serial No: **10/804,852** : Examiner: **Andrew NALVEN**
Filed: **March 19, 2004** : Group Art Unit: **2134**
For: **PRACTICAL AND SECURE STORAGE ENCRYPTION**

Mail Stop Appeal Briefs-Patents
Commission for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

APPEAL BRIEF

Sir:

This Appeal Brief is in furtherance of the Notice of Appeal filed December 4, 2008, appealing from the final Office Action mailed September 8, 2008, and in response to the Notice of Panel Decision dated January 12, 2009.

I. REAL PARTY IN INTEREST (37 C.F.R. § 41.37(c)(1)(i))

The real party in interest in this appeal is Nokia Corporation, a corporation organized under the laws of Finland.

II. RELATED APPEALS AND INTERFERENCES (37 C.F.R. § 41.37(c)(1)(ii))

There are no related appeals or interferences.

III. STATUS OF CLAIMS (37 C.F.R. § 41.37(c)(1)(iii))

Claims 1 and 4-12 are pending in the application, and claims 2-3 and 13-14 have been cancelled. Claims 1 and 4-12 are rejected, and the rejection of claims 1 and 4-12 is being appealed.

IV. STATUS OF AMENDMENTS (37 C.F.R. § 41.37(c)(1)(iv))

No amendments were filed after the final Office Action of September 8, 2008.

V. SUMMARY OF CLAIMED SUBJECT MATTER (37 C.F.R. § 41.37(c)(1)(v))

The independent claims are claim 1 and 12. Independent claim 1 is directed to an electronic device that includes an accelerator (311) configured to accelerate cryptographic data processing operations. *See* specification page 3, lines 15-16; page 11, lines 31-33; Fig. 3. The accelerator includes a first logical interface over which data to be processed is provided. *See* specification page 11, line 35—page 12, line 2; page 12, lines 32-35. A secure second logical interface over which cryptographic keys employed in processing data is provided. *See* specification page 12, lines 2-6. The first logical interface and the secure second logical interface share a same physical interface (312). *See* Fig. 3. The electronic device of claim 1 also includes a configuration register (313) configured to indicate to the accelerator whether secure mode or normal mode is set by a processor (303) arranged in the device. *See* specification page 12, lines 7-10; Fig. 3. The configuration register is also configured to receive mode setting instructions from a protected application. *See* specification page 12, lines 13-17.

Independent claim 12 is directed to a device for acceleration of data processing operations. *See* specification page 3, lines 15-16. The device includes a first logical interface (412) over which data to be processed is provided. *See* specification page 13, lines 11-14; Fig. 4. The device also includes a secure second logical (414) interface over which cryptographic keys employed in processing said data is provided. *See* specification page 13, lines 15-18. The first logical interface and the secure second logical interface share a same physical interface. The device also includes a configuration register configured to indicate to the device whether secure mode or normal mode is set by a processor arranged in the device. *See* specification page 13, line 34—page 14, line 3. The configuration register is also configured to receive mode setting instructions from a protected application. *See* specification page 13, lines 29-33.

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL (37 C.F.R. § 41.37(c)(1)(vi))

Claims 1 and 4-12 are rejected under 35 U.S.C. § 103(a) as unpatentable over *Grohoski et al.* (U.S. Appl. Publ. No. 2004/0225885) in view of *Srinivasan et al.* (U.S. Appl. Publ. No. 2004/0158742).

VII. ARGUMENT (37 C.F.R. § 41.37(c)(1)(vii))

Rejection under § 103(a) over U.S. Appl. Publ. No. 2004/0225885 in view of U.S. Appl. Publ. No. 2004/0158742

Claim 1

Appellant respectfully submits that the cited references, alone or in combination, fail to disclose or suggest all of the limitations recited in claim 1. Appellant respectfully submits that the cited references at least fail to disclose or suggest that the configuration register is configured to receive mode setting instructions from a protected application.

On page 4 of the Office Action, the Office acknowledges that *Grohoski* fails to disclose a configuration register configured to receive mode setting instructions from a protected application, and relies upon *Srinivasan* for this teaching. However, *Srinivasan* also fails to disclose or suggest that the configuration register is configured to receive mode setting instructions from a protected application, as recited in claim 1. In contrast to claim 1, *Srinivasan* only discloses that in a step (216) the trusted server optionally verifies that the secure processor (110) is authorized to receive application software from the trusted server. *See Srinivasan* paragraph [0105]. However, *Srinivasan* further states that the CPU operating in secure mode receives the application software or other additional instructions from the trusted server. *See Srinivasan* paragraph [0107]. If the CPU is already operating in a secure mode before the application software is received from the trusted server, then the application software cannot be considered to be a protected application that provides mode setting instructions to a configuration register, as recited in claim 1.

Appellant has previously argued that *Srinivasan* does not disclose that the secure mode of the processor is set by a protected application. In response, the Office alleges that the application software is assured to be executed securely by the secure processor, and therefore the application software is equal to the protected application. However, as discussed in the present application, a protected application is typically a small-size application for performing security critical operations inside the secure execution environment, and is allowed to handle secret cryptographic keys. Protected applications are applications that may be issued by trusted providers, in which case they must be authenticated, but they may also be issued by any third

party regardless of whether the third party is trusted or not. In the latter case, no authentication occurs.

In contrast to the present application, in *Srinivasan* applications corresponding to the protected applications recited in claim 1 are defined as “secure code” and “secure boot loader code.” See *Srinivasan* paragraph [0036]. These protected applications are not the equivalent to the “application software,” which the Office asserts corresponds to the protected applications recited in claim 1. *Srinivasan* defines “application software” as a set of instructions or parameters capable of being executed or interpreted by a processor. See *Srinivasan* paragraph [0031]. Since both secure code and application software are defined in the Lexicography provided in *Srinivasan*, it implies that they are differentiated from each other. *Srinivasan* makes no mention that the application software is a protected application as mentioned in claim 1. Therefore, the section relied upon by the Office does not disclose a configuration register configured to receive mode setting instructions from a protected application, as recited in claim 1. Instead, these sections only disclose that the application software places parameters for a request for services in a set of selected registers, or performs an uncached read to a register. See *Srinivasan* paragraphs [0121] & [0127]. Even if the application software are considered to be a protected application, which appellant does not admit, the functions performed by the application software in *Srinivasan* do not correspond to providing mode setting instructions, as recited in claim 1.

Furthermore, while *Srinivasan* defines “secure code” and “secure boot loader code” to be interpretable or executable by the secure processor, and known to the secure processor to be trustable, the secure code and secure boot loader code do not provide mode setting instructions to a configuration register. Claim 1 recites that the configuration register is configured to receive mode setting instructions from a protected application, however even if the secure code and secure boot loader code are considered to correspond to the protected application, *Srinivasan* does not disclose a configuration register configured to receive mode setting instructions from the secure code or the secure boot loader code. Instead, after power on of the secure processor (110) a reset signal (A170) is asserted that indicates that the secure processor (110) has been reset. See *Srinivasan* paragraph [0088]. As a result, the secure mode active signal (A160) is asserted and the CPU transfers execution control to the secure boot code (A115). The secure

mode active signal (A160) indicates to the non-volatile memory that the CPU is allowed to access the secure boot code, execute its instruction, and read and write data using the security information (113). *See Srinivasan* paragraph [0089]. However, *Srinivasan* does not disclose or suggest that a configuration register receives mode setting instructions from a protected application, instead it appears that the reset signal (A170) is responsible for setting the secure processor (110). Therefore, for at least these reasons claim 1 is not disclosed or suggested by the cited references.

Claims 4-5

Claims 4 and 5 ultimately depend from independent claim 1, and therefore are not disclosed or suggested by the cited references at least in view of their dependencies. *See In re Fine*, 5 USPQ2d 1596, 1600 (Fed. Cir. 1988) (if an independent claim is nonobvious under 35 U.S.C. 103, then any claim depending therefrom is nonobvious).

Claim 6

Appellant respectfully submits that claim 6 is not disclosed or suggested by the cited references, because the cited references at least fail to disclose or suggest that a first logical interface is configured that it is accessible by any application, and a secure second logical interface is configured such that it is accessible by protected applications only. In contrast to claim 6, *Srinivasan* only discloses that a secure processor includes two modes of operation, a monitored mode and a secure mode. The monitored mode executes the application software transparently to that application software, and the secure mode verifies that execution of the application software is authorized. *See Srinivasan* paragraph [0007]. However, even if *Srinivasan* discloses protected applications as recited in claim 6, which *Srinivasan* does not, for at least the reasons discussed above with respect to claim 1. Instead, *Srinivasan* only mentions that in the secure mode execution of the application software is authorized and does not disclose or suggest that the secure processor has a logical interface that is accessible by the application software only. In fact, *Srinivasan* states that the secure processor appears hardware-identical to the application software. *See Srinivasan* paragraph [0007]. Furthermore, *Srinivasan* only mentions that an application performs an uncached read to a register in secure mode logic, which

arms the secure mode logic to conditionally enter secure mode if and only if it encounters a subsequent read from NMI reset location. *See Srinivasan* paragraph [0127]. However, *Srinivasan* never discloses or suggests that a secure second logical interface is accessible by protected applications only, as recited in claim 6. Therefore, for at least these reasons, claim 6 is not disclosed or suggested by *Srinivasan*.

In addition, claim 6 ultimately depends from independent claim 1, and therefore is not disclosed or suggested by the cited references at least in view of its dependency. *See In re Fine*, 5 USPQ2d at 1600.

Claims 7 and 8

Claims 7 and 8 ultimately depend from independent claim 1, and therefore are not disclosed or suggested by the cited references at least in view of their dependencies. *See In re Fine*, 5 USPQ2d at 1600. Furthermore, in rejecting claim 8 the Office cites sections of *Aaro*, but does not cite *Aaro* in Section 4 of the Office Action rejecting the claims. Therefore, appellant respectfully requests that the Office correct this error in the Examiner's Answer so that appellant can accurately address the rejection to claim 8.

Claim 9

Appellant respectfully submits that claim 9 is not disclosed or suggested by the cited references, because the cited references at least fail to disclose or suggest that the processor is capable of accessing the secure second logical interface of the accelerator when the secure processor operating mode is set. *Srinivasan* only discloses that application software places parameters for a request for services in a set of selected registers in the secure mode logic, and that a register in the secure mode logic is reserved to indicate the reason for entry into secure mode. *See Srinivasan* paragraphs [0121] & [0133]. However, this is not the equivalent of the limitations recited in claim 9, because *Srinivasan* makes no mention of a secure second logical interface as recited in claim 9. Therefore, for at least this reason claim 9 is not disclosed or suggested by the cited references.

In addition, claim 9 ultimately depends from independent claim 1, and therefore is not disclosed or suggested by the cited references at least in view of its dependency. *See In re Fine*, 5 USPQ2d at 1600.

Claims 10 and 11

Claims 10 and 11 ultimately depend from independent claim 1, and therefore are not disclosed or suggested by the cited references at least in view of their dependencies. *See In re Fine*, 5 USPQ2d at 1600.

Claim 12

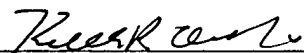
Independent claim 12 contains limitations similar to those recited in claim 1, and therefore for at least the reasons discussed above with respect to claim 1, claim 12 is not disclosed or suggested by the cited references.

Conclusion

For the reasons discussed above, appellant respectfully submits that the rejections of the final Office Action have been shown to be inapplicable, and respectfully requests that the Board reverses the rejections to pending claims 1 and 4-12. If any additional fee is required for submission of this Appeal Brief, the Commissioner is hereby authorized to charge Deposit Account No. 23-0442.

Respectfully submitted:

Date: 5 February, 2019



Keith R. Obert
Attorney for Appellant
Registration No. 58,051

WARE, FRESSOLA, VAN DER SLUYS &
ADOLPHSON, LLP
755 Main Street, PO Box 224
Monroe, CT 06468
Telephone: 203-261-1234
Facsimile: 203-261-5676
USPTO Customer No. 004955

CLAIMS APPENDIX

The claims involved in the appeal are as follows:

1. An electronic device, comprising:
an accelerator configured to accelerate cryptographic data processing operations, which accelerator comprises:
a first logical interface over which data to be processed is provided, and
a secure second logical interface over which cryptographic keys employed in processing data is provided, wherein the first logical interface and the secure second logical interface share a same physical interface, and said electronic device further comprises
a configuration register configured to indicate to the accelerator whether secure mode or normal mode is set by a processor, and configured to receive mode setting instructions from a protected application, wherein said processor is arranged in the electronic device.
- 2-3. (CANCELLED).
4. The device according to claim 1, wherein the configuration register further is configured such that it may be set in one of a plurality of possible encryption modes, and the accelerator is configured to operate in the encryption mode set in the register.
5. The device according to claim 1, wherein the accelerator is arranged such that the first logical interface and the secure second logical interface are provided via respective physical interfaces.
6. The device according to claim 1, wherein the first logical interface of the accelerator is configured such that it is accessible by any application, while the secure second logical interface of the accelerator is configured such that it is accessible by protected applications only.
7. The device according to claim 6, wherein the protected applications are configured to

prevent other applications from accessing the accelerator.

8. The device according to claim 6, wherein the protected applications are applications which are allowed to execute in the secure execution environment.

9. The device according to claim 1, further comprising:

storage circuitry comprising at least one storage area in which protected data relating to device security are located, and

wherein the processor is configured to be set in one of at least two different operating modes;

wherein the processor is given access to said storage area, in which said protected data are located, when a secure processor operating mode is set,

wherein the processor is denied access to said storage area when a normal processor operating mode is set; and

wherein the processor is capable of accessing the secure second logical interface of the accelerator, when the secure processor operating mode is set.

10. The device according to claim 9, wherein the processor is configured such that protected applications control the processor operation mode.

11. A mobile communication terminal comprising a device according to claim 1.

12. A device for acceleration of data processing operations, which device comprises:

a first logical interface over which data to be processed is provided; and

a secure second logical interface over which cryptographic keys employed in processing said data is provided, wherein the first logical interface and the secure second logical interface share a same physical interface, and

a configuration registered configured to indicate to the device whether secure mode or normal mode is set by a processor, and configured to receive mode setting instructions from a protected application, said processor being arranged in the device.

13-14. (CANCELLED)

EVIDENCE APPENDIX

None.



Attorney Docket No. 915-008.022
Serial No. 10/804,852

RELATED PROCEEDINGS APPENDIX

None.



Practitioner's Docket No. 915-008.022

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of: Lauri PAATERO

Application No.: 10 / 804,852

Group No.: 2134

Filed: March 19, 2004

Examiner: Andrew NALVEN

For: PRACTICAL AND SECURE

Reexamination control No.:

STORAGE ENCRYPTION

Mail Stop Appeal Brief—Patents

Commissioner for Patents

P.O. Box 1450

Alexandria, VA 22313-1450

**TRANSMITTAL OF APPEAL BRIEF
(PATENT APPLICATION OR EX PARTE REEXAMINATION—
37 C.F.R. § 41.37)**

NOTE: The phrase "the date on which" an "appeal was taken" in 35 U.S.C. 154(b)(1)(A)(ii) (which provides an adjustment of patent term if there is a delay on the part of the Office to respond within 4 months after an "appeal was taken") means the date on which an appeal brief under § 1.192 (and not a notice of appeal) was filed. Compliance with § 41.37 requires that: 1. the appeal brief fee (§ 41.20(b)(2)) be paid (§ 41.37(a)(2)); and 2. the appeal brief complies with §§ 41.73(c)(i)-(x). See Notice of September 18, 2000, 65 Fed. Reg. 56366, 56385-56387 (Comment 38).

1. Transmitted herewith is the APPEAL BRIEF in this application, with respect to the Notice of Appeal filed on December 4, 2008

NOTE: Appellant must file a brief under this section within two months from the date of filing the notice of appeal under § 41.31. 37 CFR 41.(a)(1). The brief is no longer required in triplicate. The former alternative time for filing a brief (within the time allowed for reply to the action from which the appeal was taken)

CERTIFICATION UNDER 37 C.F.R. §§ 1.8(a) and 1.10*

(When using Express Mail, the Express Mail label number is mandatory;
Express Mail certification is optional.)

I hereby certify that, on the date shown below, this correspondence is being:

MAILING

- ☒ deposited with the United States Postal Service in an envelope addressed to Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450

37 C.F.R. § 1.8(a)

37 C.F.R. § 1.10*

- ☒ with sufficient postage as first class mail.

☐ as "Express Mail Post Office to Addressee"
Mailing Label No. _____ (mandatory)

TRANSMISSION

- ☐ facsimile transmitted to the Patent and Trademark Office, (571) 273-8300.

Signature

Kathleen Sipos

(type or print name of person certifying)

Date: 2/5/09

* Only the date of filing (§ 1.6) will be the date used in a patent term adjustment calculation, although the date on any certificate of mailing or transmission under § 1.8 continues to be taken into account in determining timeliness. See § 1.703(f). Consider "Express Mail Post Office to Addressee" (§ 1.10) or facsimile transmission (§ 1.6(d)) for the reply to be accorded the earliest possible filing date for patent term adjustment calculations.

has been removed. Appellant must file within two months from the notice of appeal. See Notice of August 12, 2004, 69 FR 49960, 49962.

2. STATUS OF APPLICANT

This application is on behalf of

☒ other than a small entity.

☐ a small entity.

A statement:

☐ is attached.

☐ was already filed.

3. FEE FOR FILING APPEAL BRIEF

Pursuant to 37 C.F.R. § 41.20(b)(2), the fee for filing the Appeal Brief is:

☐ small entity \$ 270.00

☒ other than a small entity \$ 540.00

Appeal Brief fee due \$ 540.00

4. EXTENSION OF TERM

NOTE: 37 C.F.R. § 1.704(b) "...an applicant shall be deemed to have failed to engage in reasonable efforts to conclude processing or examination of an application for the cumulative total of any periods of time in excess of three months that are taken to reply to any notice or action by the Office making any rejection, objection, argument, or other request, measuring such three-month period from the date the notice or action was mailed or given to the applicant, in which case the period of adjustment set forth in § 1.703 shall be reduced by the number of days, if any, beginning on the day after the date that is three months after the date of mailing or transmission of the Office communication notifying the applicant of the rejection, objection, argument, or other request and ending on the date the reply was filed. The period, or shortened statutory period, for reply that is set in the Office action or notice has no effect on the three-month period set forth in this paragraph."

NOTE: The time periods set forth in 37 C.F.R. § 1.192(a) are subject to the provision of § 1.136 for patent applications. 37 C.F.R. § 1.191(d). See also Notice of November 5, 1985 (1060 O.G. 27).

NOTE: As the two-month period set in § 1.192(a) for filing an appeal brief is not subject to the six-month maximum period specified in 35 U.S.C. § 133, the period for filing an appeal brief may be extended up to seven months. 62 Fed. Reg. 53,131, at 53,156; 1203 O.G. 63, at 84 (Oct. 10, 1997).

☐ The proceedings herein are for a patent application and the provisions of 37 C.F.R. § 1.136 apply.

WARNING: The provisions of 37 CFR § 1.136 do not apply in an ex parte reexamination. Any requests for extension must be made pursuant to 37 CFR 1.550(c).

(complete (a) or (b), as applicable)

(a) ☐ Applicant petitions for an extension of time under 37 C.F.R. § 1.136 (fees: 37 C.F.R. § 1.17(a)(1)-(5)) for the total number of months checked below:

Extension (months)	Fee for other than small entity	Fee for small entity
<input type="checkbox"/> one month	\$ 130.00	\$ 65.00
<input type="checkbox"/> two months	\$ 490.00	\$ 245.00
<input type="checkbox"/> three months	\$ 1,110.00	\$ 555.00
<input type="checkbox"/> four months	\$ 1,730.00	\$ 865.00
<input type="checkbox"/> five months	\$ 2,350.00	\$ 1,175.00

Fee: \$ _____

If an additional extension of time is required, please consider this a petition therefor.

(check and complete the next item, if applicable)

- ☐ An extension for _____ months has already been secured, and the fee paid therefor of \$ _____ is deducted from the total fee due for the total months of extension now requested.

Extension fee due with this request \$ _____

or

- (b) ☒ Applicant believes that no extension of term is required. However, this conditional petition is being made to provide for the possibility that applicant has inadvertently overlooked the need for a petition and fee for extension of time.

5. TOTAL FEE DUE

The total fee due is:

Appeal brief fee \$ 540.00

Extension fee (if any) \$ _____

TOTAL FEE DUE \$ 540.00

6. FEE PAYMENT

☒ Attached is a ☒ check ☐ money order in the amount of \$ 540.00

☐ Authorization is hereby made to charge the amount of \$ _____

☐ to Deposit Account No. _____

☐ to Credit card as shown on the attached credit card information authorization form PTO-2038.

WARNING: Credit card information should not be included on this form as it may become public.

☐ Charge any additional fees required by this paper or credit any overpayment in the manner authorized above.

☐ A duplicate of this paper is attached.

7. FEE DEFICIENCY

NOTE: If there is a fee deficiency and there is no authorization to charge an account, additional fees are necessary to cover the additional time consumed in making up the original deficiency. If the maximum six-month period has expired before the deficiency is noted and corrected, the application is held abandoned. In those instances where authorization to charge is included, processing delays are encountered in returning the papers to the PTO Finance Branch in order to apply these charges prior to action on the cases. Authorization to change the deposit account for any fee deficiency should be checked. See the Notice of April 7, 1986, 1065 O.G. 31-33.

☒ If any additional extension and/or fee is required,

AND/OR

☒ If any additional fee for claims is required, charge:

☒ Deposit Account No. 23-0442

☐ Credit card as shown on the attached credit card information authorization form PTO-2038.

WARNING: Credit card information should not be included on this form as it may become public.



Date: February 5, 2009

Reg. No.: 58,051

Customer No.: 004955

Keith R. Obert

SIGNATURE OF PRACTITIONER

Keith R. Obert of Ware, Fressola,

Van Der Sluys & Adolphson, LLP

(type or print name of practitioner)

P.O. Box 224

P.O. Address

Monroe, CT 06468

(Transmittal of Appeal Brief [9-6.1]—page 4 of 5)